Jw

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,310	07/11/2001	Handong Wu	NETAP011	2093

28875 7590 03/15/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
JEAN GILLES, JUDE	
ART UNIT	**PAPER NUMBER**
2143	

DATE MAILED: 03/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No. 09/904,310	Applicant(s) WU ET AL.	
	Examiner Jude J Jean-Gilles	Art Unit 2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *22 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-24 and 26-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-24 and 26-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/7/02*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

This Action is in regards to the Reply received on 22 December, 2004.

Response to Amendment

1. This action is responsive to the application filed on December 22^{nd}, 2004. Claims 1, 15, 20, 22, and 26 were amended. Claims 5, 6, and 25 were cancelled. Claims 30 and 31 are newly added. Claims 1-31 are pending. Claims 1-31 represent a method and system for "Protecting Internet Protocol Addresses."

Response to Arguments

2. Applicant's arguments with respect to former claims 5 and 6 (now substantially incorporated into each of the independent claims 1, 15, 20, 22, and 26 have been carefully considered, but are not deemed fully persuasive. Applicant's arguments are deemed moot in view of the following new ground of rejection as explained here below, necessitated by Applicant substantial amendment (i.e., incorporating former claims 5 and 6 into each of claims 1, 15, 20, 22, and 26) to the claims which significantly affected the scope thereof.

The dependent claims stand rejected as articulated in the First Office Action and all objections not addressed in Applicant's response are herein reiterated. New claims 30 and 31 have been considered and are rejected in view of new ground of rejection.

Information Disclosure Statement

3. The references listed on the Information Disclosure Statement submitted on 01/11/2002 have been considered by the examiner (see attached PTO-1449A).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-4, 7-24, and 26-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over Redlich (Redlich), U.S. Patent No. 6,591,306 B1 in view of Belissent (Belissent), U.S. No. 6,789,203 B1.

Regarding **claim 1,** Redlich discloses the invention substantially as claimed. Redlich teaches a method for protecting a host located within a computer network (*fig. 18, item 200*), the method comprising:

mapping a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network (*column 16, lines 15-24; note that the guess station is the public host and that the local stations are the local hosts*), said public host address being available from a domain name system server (*column 28, lines 47-52; note that appointment of a couple of DNS servers on the guest's home network*);

receiving a request for communication with the secret host at the public host (*column 18, lines 57-67; column 19, lines 1-10*);

forwarding said request from the public host to the secret host (*column 19, lines 11-15*); and

processing said request at the secret host and communicating from the secret host over the network, wherein said communication appears to be sent from the public host (*column 20, lines 25-36*); However, Redlich does not specifically disclose a method <u>wherein forwarding said request comprises:</u>

<u>determining whether an attack is consuming significant resources,</u>

<u>if it is determined that an attack is not consuming significant resources slowing down the forwarding of said request short of stopping the same, and</u>

<u>if it is determined that an attack is consuming significant resources. stopping the forwarding of said request.</u>

In the same field of endeavor, Belissent teaches "*a denial of service attack incident where the attacker seeks to use a substantial amount of server resources*" [see Belissent, column 2, lines 13-38; fig. 2, item 202]. Belissent further discloses a rejection threshold whereas, the consumption of resources is expressed in terms of the number of connections attempts recorded per client IP address recorded in memory [see Belissent, column 5, lines 62-67; column 6, lines 1-17]. In addition Belissent discloses a "*slowdown threshold in which, the IP throttler unit 216 slows down the connection request rate stream by what is referred to as the wait time*" [see Belissent, column 6,

lines 17-56] and "*if it determined that the increment is greater than the connection threshold, the connection request is rejected*" [see Belissent, column 7, lines 1-17]

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Belissent's teachings of slowing down and blocking the forwarding of request from the attacker with the teachings of Redlich, for the purpose of improving the ability of a local network "*to provide for security against malicious intrusion or attacks from a foreign network*" as stated by Redlich in lines 34-36 of column 14. Belissent also provides motivation to combine disclosing "*a system design to either artificially slowing down or by refusing request for processing*" [see Belissent, column 4, lines 12-22]. By this rationale, **claim 1** is rejected.

Regarding **claim 2,** the combination of Redlich-Belissent teaches the method of claim 1 wherein the network is the Internet and the secret host is a server [*see Redlich, column 25, lines 12-59*]. The same motivation that was used for claim 1, also applies to claim 2 [see Redlich, column 14, lines 26-33]. By this rationale, **claim 2** is rejected.

Regarding **claim 3,** the combination of Redlich-Belissent teaches the method of claim 2 wherein the server hosts a Web site [*see Redlich, column 29, lines 49-59*]. The same motivation that was used for claim 1, also applies to claim 3 [see Redlich, column 14, lines 26-33]. By this rationale, **claim 3** is rejected.

Regarding **claim 4,** the combination of Redlich-Belissent teaches the method of claim 1 wherein receiving a request comprises receiving a URL at the domain name system server, the domain name system server providing an IP address of the public

host corresponding to the URL [*see Redlich, column 29, lines 49-59*]. The same motivation that was used for claim 1, also applies to claim 4 [see Redlich, column 14, lines 26-33]. By this rationale, **claim 4** is rejected.

Regarding **claim 7,** the combination Redlich- Belissent teaches the method of claim 1 further comprising notifying the secret host of the attack [*see* Belissent, *column 4, lines 9-25*].]. The same motivation that was used for claim 1, also applies to claim 7 [see Redlich, column 14, lines 26-33]. By this rationale **claim 7** is rejected.

Regarding **claim 8**, the combination Redlich- Belissent teaches the method of claim 7 further comprising tracking down a source of the attack [*see* Redlich, *column 24, lines 19-33*].]. The same motivation that was used for claim 1, also applies to claim 8 [see Redlich, column 14, lines 26-33]. By this rationale **claim 8** is rejected.

Regarding **claim 9**, the combination Redlich- Belissent teaches the method of claim 8 wherein tracking down a source of the attack comprises performing a trace back at the secret host [*see* Redlich, *column 24, lines 19-63*].]. The same motivation that was used for claim 1, also applies to claim 9 [see Redlich, column 14, lines 26-33]. By this rationale **claim 9** is rejected.

Regarding **claim 10**, the combination Redlich- Belissent discloses the method of claim 1, further comprising directing one or more clients to send requests to an alternate path public host [*see* Redlich, *column 24, lines 46-63*]. The same motivation that was used for claim 1, also applies to claim 10 [see Redlich, column 14, lines 26-33]. By this rationale **claim 10** is rejected.

Regarding **claim 11,** the combination Redlich- Belissent teaches the method of claim 10 wherein a notification that the public host is under attack is received at the secret host [*see Redlich, column 25, lines 12-67*]. The same motivation that was used for claim 1, also applies to claim 11 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 11** is rejected.

Regarding **claim 12,** the combination Redlich- Belissent teaches the method of claim 10 wherein a notification that the public host is congested is received at the secret host [*see Belissent, column 6, lines 18-67*]. The same motivation that was used for claim 1, also applies to claim 12 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 12** is rejected.

Regarding **claim 13,** the combination Redlich- Belissent teaches the method of claim 10 wherein the secret host has received a request for heightened security [*see Redlich, column 25, lines 19-22*]. The same motivation that was used for claim 1, also applies to claim 13 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 13** is rejected.

Regarding **claim 14,** the combination Redlich- Belissent teaches the method of claim 10 further comprising requesting the DNS server to replace the public host address with an alternate public host address [*see Redlich, column 23, lines 34-63*]. The same motivation that was used for claim 1, also applies to claim 14 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 14** is rejected.

Regarding **claim 15,** the combination Redlich- Belissent teaches a computer program product for protecting a host located within a computer network (*fig. 18, items 200, 210, 400, 502-503, and 900*), comprising:

computer code that maps a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network (*column 18, lines 16-26*), said public host address being available from a domain name system server (*column 28, lines 47-52; fig. 11, tunnel server*);

computer code that receives a request for communication with the secret host at the public host (*column 18, lines 16-34*);

computer code that forwards said request from the public host to the secret host (*column 18, lines 16-34*);

computer code that processes said request at the secret host and communicates from the secret host over the network, wherein said communication appears to be sent from the public host (*column 18, lines 16-37*); and

a computer-readable storage medium for storing the codes (*column 18, lines 25-27*).

wherein forwarding said request comprises:

determining whether an attack is consuming significant resources, [see Belissent, column 2, lines 13-38; fig. 2, item 202]

if it is determined that an attack is not consuming significant resources slowing down the forwarding of said request short of stopping the same, [see Belissent, column 5, lines 62-67; column 6, lines 1-17].and

<u>if it is determined that an attack is consuming significant resources. stopping the forwarding of said request</u> [see Belissent, column 6, lines 17-56; column 7, lines 1-17]. The same motivation that was used for claim 1, also applies to claim 15 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 15** is rejected.

Regarding **claim 16,** the combination Redlich- Belissent teaches the computer program product of claim 15 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave [see Redlich, *column 18, lines 25-27*]. The same motivation that was used for claim 1, also applies to claim 16 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 16** is rejected.

Regarding **claim 17,** the combination Redlich- Belissent teaches the computer program product of claim 15 further comprising code that receives at the secret host a notification that the public host is under attack [see Belissent, column 1, lines 40-65; fig. 1, item 106]. The same motivation that was used for claim 1, also applies to claim 17 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 17** is rejected.

Regarding **claim 18,** the combination Redlich- Belissent teaches the computer program product of claim 17 further comprising code that directs one or more clients to send requests to an alternate public host upon receiving said notification [*see Redlich, column 24, lines 53-57*]. The same motivation that was used for claim 1, also applies to claim 18 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 18** is rejected.

Regarding **claim 19,** the combination Redlich- Belissent teaches the computer program product of claim 17 further comprising code that requests the DNS server to replace the public host address with an alternate public host address upon receiving said notification [*see Redlich, column 24, lines 53-57*]. The same motivation that was used for claim 1, also applies to claim 19 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 19** is rejected.

Regarding **claim 20,** the combination Redlich- Belissent teaches a system for protecting a host located within a computer network [*see Redlich, fig. 18, items 200, 210, 400, 502-503, and 900*], the system comprising:

a public host having a public host address available from a DNS server [*see Redlich, column 28, lines 47-52*]; and

a secret host having a secret host address and containing data accessible over the computer network, said public host address being mapped to said secret host address [*see Redlich, column 16, lines 15-24*];

wherein the public host is operable to forward requests received from the network to the secret host and the secret host is Operable to process said requests and communicate from the secret host to the network with said communication appearing to be sent from the public host [*see Redlich, column 20, lines 25-36; column 19, lines 1-15*].

<u>wherein forwarding said request comprises:</u>

<u>determining whether an attack is consuming significant resources,</u> [see Belissent, column 2, lines 13-38; fig. 2, item 202]

if it is determined that an attack is not consuming significant resources slowing down the forwarding of said request short of stopping the same, [see Belissent, column 5, lines 62-67; column 6, lines 1-17].and

if it is determined that an attack is consuming significant resources. stopping the forwarding of said request [see Belissent, column 6, lines 17-56; column 7, lines 1-17]. The same motivation that was used for claim 1, also applies to claim 20 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 20** is rejected.

Regarding **claim 21,** the combination Redlich- Belissent teaches the system of claim 20 wherein the secret host is configured to manage the public host [see Redlich, *column 3, lines 62-67]*. The same motivation that was used for claim 1, also applies to claim 21 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 21** is rejected.

Regarding **claim 22,** the combination Redlich- Belissent teaches a method for hiding an IP address of a computer node located within a computer network [*see Redlich, fig. 18, items 200, 210, 400, 502-503, and 900*], the method comprising:

associating an IP address for a public node with an IP address of a secret node such that only the public node has access to the IP address of the secret node, said P address for the public node being available from a DNS server [*see Redlich, column 28, lines 47-52; note that appointment of a couple of DNS servers on the guest's home network*];

receiving packets from the network at the public node [*see Redlich,* column *18, lines 57-67; column 19, lines 1-10*];

forwarding said packets from the public node to the secret node [*see Redlich, column 19, lines 11-15*]; and

responding to said packets at the secret node such that a response appears to be sent from the public node rather than the secret node [*see Redlich, column 20, lines 25-36*].

wherein forwarding said request comprises:

determining whether an attack is consuming significant resources, [see Belissent, column 2, lines 13-38; fig. 2, item 202]

if it is determined that an attack is not consuming significant resources slowing down the forwarding of said request short of stopping the same, [see Belissent, column 5, lines 62-67; column 6, lines 1-17].and

if it is determined that an attack is consuming significant resources. stopping the forwarding of said request [see Belissent, column 6, lines 17-56; column 7, lines 1-17]. The same motivation that was used for claim 1, also applies to claim 22 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 22** is rejected.

Regarding **claim 23,** the combination Redlich- Belissent teaches the method of claim 22 wherein the packets contain requests for data and the secret node is a server hosting a Web site [*see Redlich, fig. 19, items 900, 941-942; column 28, lines 56-64; column 29, lines 49-59*]. The same motivation that was used for claim 1, also applies to claim 23 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 23** is rejected.

Regarding **claim 24,** the combination Redlich- Belissent teaches the method of claim 22 wherein the packets contain e-mail [*see Redlich, column 16, lines 45-51*]. The same motivation that was used for claim 1, also applies to claim 24 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 24** is rejected.

Regarding **claim 26,** the combination Redlich- Belissent teaches the method of claim 22 further comprising requesting the DNS server to replace the IP address of the public node with an IP address of an alternate public node [*see Redlich, column 23, lines 34-63*]. The same motivation that was used for claim 1, also applies to claim 26 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 26** is rejected.

Regarding **claim 27,** the combination Redlich- Belissent teaches the method of claim 22 further comprising directing specific client computers to send packets directed at the public node to an alternate public node [*see Redlich, column 23, lines 34-63*]. The same motivation that was used for claim 1, also applies to claim 27 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 27** is rejected.

Regarding **claim 28,** the combination Redlich- Belissent teaches the method of claim 22 further comprising switching to an alternate public host when congestion at the public host exceeds a predetermined level [*see Belissent, column 6, lines 18-67*]. The same motivation that was used for claim 1, also applies to claim 28 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 28** is rejected.

Regarding **claim 29,** the combination Redlich- Belissent teaches the method of claim 22 further comprising switching to an alternate public host to provide increased security at the secret host [*see Redlich, column 25, lines 19-22*]. The same motivation that was used for claim 1, also applies to claim 29 [*see Redlich, column 14, lines 26-33*]. By this rationale **claim 29** is rejected.

6. **Claims 30 and 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Redlich and Belissent, in view of Shostack et al (Shostack), U.S. No. 6,298,445 B1.

Regarding **claim 30,** the combination Redlich- Belissent discloses the invention substantially as claimed. Redlich- Belissent teaches the method of hiding an IP address of a computer node located within a computer network of claim 22 wherein, after stopping the forwarding of said packets, said secret node requests that the DNS server replace a current public node IP address with, an IP address of an alternate public node, and attempts to track down a source of the attack [see claim 22 above]. However, the combination does not disclose specifically a method where, after the attack has stopped, an IP address of an alternate Post Office Box Internet Protocol (POBIP) node is replaced with an original public node IP address.

In the same field of endeavor, Shostack discloses " *a push mechanism that utilizes a POP mail server to hold mail for the user in the public network (node) and alternatively the mail will be push onto the user's local computer*" [see Shostack, column 8, lines 42-67, column 9, lines 1-24].

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Shostack's teachings of the Post Office Box Protocol with the teachings of Redlich-Belissent, for the purpose of improving the ability of a local network "*to provide for security against malicious intrusion or attacks from a foreign network*" as stated by Redlich in lines 34-36 of column 14. Shostack also provides motivation to combine disclosing "*to make the network les vulnerable to attacks"* [see Shostack, column 2, lines 20-24]. By this rationale, **claim 30** is rejected.

Regarding **claim 31,** the combination Redlich- Belissent- Shostack teaches the method of claim 22 wherein, after stopping the forwarding of said packets. said secret node notifies select clients of an alternate public node IP address, and attempts to track down a source of the attack [see claim 22 above], where, after the attack has stopped, an IP address of an alternate Post Office Box Internet Protocol IPOBDI node is replaced with the IP address of the public node [see Shostack, column 8, lines 42-67, column 9, lines 1-24]. The same motivation that was used for claim 30, also applies to claim 31 [see Shostack, column 2, lines 20-24]. By this rationale **claim 31** is rejected.

Response to Arguments

7. Applicant's Request for Reconsideration filed on December 22nd, 2004 has been carefully considered but is not deemed fully persuasive. However, because there exists the likelihood of future presentation of this argument, the Examiner thinks that it is prudent to address Applicants' main points of contention.

A. Applicant asserts that only applicant teaches and claims a two-sprung response (including stopping and slowing) based, specifically, on a determination as to whether an attack is consuming significant resources, as claimed in independent **claims 1, 15, 20 and 22**.

B. Applicant contends that at least the first and third element of prima facie case of obviousness has not been met. Not all the limitations are taught by the references.

C. Applicant further assertion that the Examiner's application of the prior art is replete with deficiencies . For example :

1. " *tracking down the source of attack comprises a trace back at the secret host*".

2. "*code that directs one or more clients to send requests to an alternate public host upon receiving said notification*".

3. "*the secret host is configured to manage to public host*".

4. "*congestion at the public host exceeds a predetermined level and that a switching is required to an alternate public host*".

D. Applicant bring to the Examiner's attention the following additional dependent claims that have been added for full consideration.

8. As to "Point A" it is the position of the Examiner that the two-sprung response is taught by Belissent and that the prima facie case of obviousness is established as there is clear motivation to combine Redlich and Belissent with a reasonable expectation of success [see examination of independent claims 1, 15, 20, and 22 above]. As a result, Applicant's arguments are deemed moot in view of the following new grounds of rejection.

As to "Point B", the Applicant rightfully notes the suggestion to combine from Underwood is weak and as a result, the Examiner has reestablished the prima facie case of obviousness over Redlich in view of Belissent and has covered all three grounds for rejection under 103(a) as required by the office.

As to point C, all dependent claims limitations considered under the new grounds for rejection under and the 103(a) stand rejected as articulated in the First Office Action.

As to point D, the new dependent claims have been rejected over Redlich and Belissent in view of Shostack. All rejections not addressed in the Applicant response are herein reiterated

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from examiner should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914. The examiner can normally be reached on Monday-Thursday and every other Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley, can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is (703) 305-3719.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jude Jean-Gilles

Patent Examiner

Art Unit 2143

BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER

JJG

February 283, 2005